ACTA ARITHMETICA
104.2 (2002)

Bounds for quadratic Waring's problem

by

Myung-Hwan Kim (Seoul) and Byeong-Kweon Oh (Columbus, OH)

1. Introduction. In 1770, Lagrange [L] proved the famous four square theorem, i.e., for every positive integer n, there exists an integer solution of the equation

$$x^2 + y^2 + z^2 + w^2 = n.$$

After Lagrange, this theorem was generalized in many directions. One interesting generalizations concerns the so-called *new* (or *quadratic*) *Waring's problem* due to L. J. Mordell [M1], which is about sums of squares that represent all positive integral quadratic forms of given rank. In particular, Mordell proved that every binary positive integral quadratic form can be represented by a sum of five squares. Later, C. Ko [K1] proved that every ternary (quaternary or quinary) positive integral quadratic form can be represented by a sum of six (seven or eight, respectively) squares. So, they naturally expected that every positive n-ary integral quadratic form could be represented by a sum of $n + 3$ squares. This, however, turned out to be false. The quadratic form defined by the root lattice E_6 cannot be represented by sums of squares (see [M2], [CS2] and [Pl]). After Mordell found this, several authors tried to determine the minimum number $g[n]$ of squares whose sum represents all positive integral quadratic forms of rank n that are representable by sums of squares.

We adopt lattice-theoretic language. A $\mathbb{Z}$-*lattice* L is a finitely generated free $\mathbb{Z}$-module in $\mathbb{R}^n$ equipped with a non-degenerate symmetric bilinear form B such that $B(L, L) \subset \mathbb{Z}$. The corresponding quadratic map is denoted by Q, i.e., $Q(\mathbf{e}) = B(\mathbf{e}, \mathbf{e})$ for every $\mathbf{e} \in L$. The ideal of $\mathbb{Z}$ generated by $B(\mathbf{e}_i, \mathbf{e}_j)$'s is called the *scale* of L, denoted by $\mathfrak{s}(L)$. For a $\mathbb{Z}$-lattice

$$L = \mathbb{Z}\mathbf{e}_1 + \ldots + \mathbb{Z}\mathbf{e}_m$$

2000 *Mathematics Subject Classification*: 11E12, 11E06.

Key words and phrases: quadratic Waring's problem, representations by sums of squares.

The first author was supported in part by KOSEF Research Fund (00-0701-01-5-2).

with basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$, we define the corresponding matrix

$$M_L := (B(\mathbf{e}_i, \mathbf{e}_j)),$$

which is an $m \times m$ symmetric integer matrix. We often identify a $\mathbb{Z}$-lattice L with its corresponding matrix M_L. If M_L is diagonal, we often write

$$L = \langle Q(\mathbf{e}_1), \ldots, Q(\mathbf{e}_n)\rangle = \langle Q(\mathbf{e}_1)\rangle \perp \ldots \perp \langle Q(\mathbf{e}_n)\rangle.$$

For $a \in \mathbb{R}^\times$, we let

$$aL := \mathbb{Z}(a\mathbf{e}_1) + \ldots + \mathbb{Z}(a\mathbf{e}_n).$$

The lattice $\mathbb{Z}^n$ equipped with the standard inner product is denoted by I_n. A $\mathbb{Z}$-lattice L is said to be *positive definite* or simply *positive* if $Q(\mathbf{e}) > 0$ for every $\mathbf{e} \in L, \mathbf{e} \neq \mathbf{0}$. In this paper, we always assume the following unless stated otherwise:

(1) *Every $\mathbb{Z}$-lattice considered is positive definite.*

A $\mathbb{Z}$-lattice L is said to be *even* when $Q(L) \subset 2\mathbb{Z}$, and *odd*, otherwise. As usual,

$$\det L := \det(B(\mathbf{e}_i, \mathbf{e}_j))$$

is called the *discriminant* of L. A $\mathbb{Z}$-lattice L is said to be *unimodular* if $\det L = 1$. For a $\mathbb{Z}$-lattice L and a prime p,

$$L_p := \mathbb{Z}_p L = \mathbb{Z}_p \otimes_{\mathbb{Z}} L$$

is a $\mathbb{Z}_p$-lattice called the *localization* of L at p, where $\mathbb{Z}_p$ is the p-adic integer ring.

Let ℓ, L be $\mathbb{Z}$-lattices. We say that L *represents* ℓ if there is an injective $\mathbb{Z}$-linear map from ℓ into L that preserves the bilinear forms, and write $\ell \to L$. Such a map is called a *representation*. A representation is called an *isometry* if it is surjective. We say that ℓ and L are *isometric* and write $\ell \simeq L$ if there exists an isometry between them. For a $\mathbb{Z}$-lattice L, we define the *class* and *genus* of L by

$$\begin{aligned}\mathrm{cls}(L) &:= \{K : \mathbb{Z}\text{-lattice} \mid K \simeq L \text{ over } \mathbb{Z}\},\\ \mathrm{gen}(L) &:= \{K : \mathbb{Z}\text{-lattice} \mid K_p \simeq L_p \text{ over } \mathbb{Z}_p \text{ for all } p\}.\end{aligned}$$

It is well known that $\mathrm{gen}(L)$ contains a finite number of distinct classes. This number is called the *class number* of L, denoted by $h(L)$. If $\ell_p \to L_p$ for all p, or equivalently $\ell \to \mathrm{gen}(L)$, then it is known that $\ell \to K$ for some $K \in \mathrm{gen}(L)$.

Let

$$\mathfrak{S}_n := \{\ell : \mathbb{Z}\text{-lattice} \mid \ell \to I_g \text{ for some } g, \mathrm{rank}(\ell) = n\},$$

and

(2) $$g[n] := \min\{g \mid \ell \to I_g \text{ for every } \ell \in \mathfrak{S}_n\}.$$

Applying the results in [HKK], one can easily prove that $g[n]$ exists for all n. The four-square theorem of Lagrange, and the results of Mordell and Ko mentioned above can be summarized as follows:

$$g[n] = n + 3 \quad \text{for } 1 \le n \le 5. \tag{3}$$

In fact, this is an immediate consequence of the fact that the class number of I_n is 1 for $1 \le n \le 8$ and of the local representation theory. The following question arises quite naturally:

$$\textit{Is} \quad g[n] = n + 3 \quad \textit{for all } n \ge 1\textit{?}$$

Concerning this question, Ko conjectured in [K2] that $g[6] = 9$. However, the authors proved recently [KO1,2] that

$$g[n] \ge \lfloor 3n/2 \rfloor + 1 > n + 3 \quad \text{for all } n \ge 6, \quad g[6] = 10. \tag{4}$$

The first explicit upper bound for $g[n]$ was given by Icaza [Ic]. She obtained her bound by computing the so-called HKK-constant. But her bound is huge containing a factor

$$n^{n+1} 2^{4h(I_{n+3})},$$

where $h(I_n) = n^{\Theta(n^2)}$. Recently, the authors improved the bounds of $g[n]$ as follows:

$$2n - \lceil \log_2 n \rceil - 2 \le g[n] \le 3 \cdot 3^{n/2}\, \tau_{n+3} + n + 4 \tag{5}$$

for $n \ge 14$ where

$$\tau_k := \sum_{i=17}^{k} \lfloor 2 \log_2 i \rfloor - k + 18 = O(k \log k)$$

for $k \ge 17$ (see [KO3]). For small n's, Oh [Oh] proved

$$g[n] \le n(n+1)/2 + n + 3 \tag{6}$$

for $7 \le n \le 11$, and Sasaki [Sa] recently showed that:

$$g[n] \le \begin{cases} 2 \cdot 3^n + n + 6 & \text{for } 12 \le n \le 13, \\ 3 \cdot 4^n + n + 3 & \text{for } 14 \le n \le 20, \end{cases} \qquad g[7] \le 25. \tag{7}$$

In this article, we provide sharper bounds of $g[n]$ for $12 \le n \le 20$. More precisely, we prove

$$g[n] \le 5n^3/2 \tag{8}$$

for $12 \le n \le 20$. We also prove

$$11 \le g[7] \le 24, \quad 13 \le g[8] \le 37. \tag{9}$$

For the minimal rank $u[n]$ among the ranks of all positive $\mathbb{Z}$-lattices L that represent all n-ary positive $\mathbb{Z}$-lattices, see [KKO]. Finally, we refer the readers to O'Meara [O'M1], Conway and Sloane [CS1] for unexplained terminology, notation, and basic facts about $\mathbb{Z}$-lattices.

2. Lemmas. Let $\ell = \mathbb{Z}\mathbf{x}_1 + \ldots + \mathbb{Z}\mathbf{x}_n \subset I_g$ be a $\mathbb{Z}$-lattice, where $\mathbf{x}_i = (a_{i1}, \ldots, a_{ig})$ for $1 \le i \le n$. For $1 \le j \le g$, define

$$\mathbf{v}_j := {}^{\mathrm{t}}(a_{1j}, a_{2j}, \ldots, a_{nj}),$$

where ${}^{\mathrm{t}}A$ is the transpose of a matrix or a vector A. Since these $\mathbf{v}_j$'s also characterize ℓ, we may write

$$\ell = \mathbb{Z}\text{-span}_n(\mathbf{v}_1, \ldots, \mathbf{v}_g) \subset I_g, \tag{10}$$

where $\mathbb{Z}\text{-span}_n(\mathbf{v}_1, \ldots, \mathbf{v}_g)$ denotes the lattice spanned over $\mathbb{Z}$ by the n-vectors $\mathbf{v}_1, \ldots, \mathbf{v}_g$. Note that for positive integers $s_1, \ldots, s_g$,

$$\widetilde{\ell} = \mathbb{Z}\text{-span}_n(\overbrace{\mathbf{v}_1, \ldots, \mathbf{v}_1}^{s_1 \text{ times}}, \ldots, \overbrace{\mathbf{v}_g, \ldots, \mathbf{v}_g}^{s_g \text{ times}}) \subset I_{s_1+\ldots+s_g}$$

of rank n is represented by the $\mathbb{Z}$-lattice $\langle s_1 \rangle \perp \ldots \perp \langle s_g \rangle$ of rank g.

Conway and Sloane [CS2] called a $\mathbb{Z}$-lattice ℓ of rank n *s-integrable* if $\sqrt{s}\,\ell$ can be represented by a sum of squares, i.e., $\sqrt{s}\,\ell \in \mathfrak{S}_n$, where s is a positive integer. Define

$$\phi(s) := \min\{n \mid \exists \text{ a } \mathbb{Z}\text{-lattice } \ell \text{ of rank } n \text{ such that } \sqrt{s}\,\ell \notin \mathfrak{S}_n\}. \tag{11}$$

It is known [CS2], [KO3] that

$$\phi(1) = 6, \quad \phi(2) = 12, \quad \phi(3) = 14, \ \ldots \tag{12}$$

and that for large enough s,

$$\phi(s) > \frac{\ln s}{8 \ln \ln s}. \tag{13}$$

Let $\mathbb{F}_2 = \{0, 1\}$ be the field of 2 elements and $\mathrm{Sym}_n(\mathbb{F}_2)$ be the set of all $n \times n$ symmetric matrices over $\mathbb{F}_2$. For a vector $\mathbf{a} = (a_1, \ldots, a_g) \in \mathbb{F}_2^g$, we define $\mathrm{wt}(\mathbf{a})$, the *weight* of $\mathbf{a}$, to be the number of indices i such that $a_i = 1$.

LEMMA 2.1. *Let V be an m-dimensional subspace of $\mathbb{F}_2^g$. Then there exists $\mathbf{x} \in V$ such that* $\mathrm{wt}(\mathbf{x}) \ge m$.

Proof. Let $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ be a basis of V, where $\mathbf{u}_i = (u_{i1}, \ldots, u_{ig})$ for $i = 1, \ldots, m$. Then reduce the $m \times g$ matrix $U = (u_{ij})$ to the row echelon matrix U' by applying elementary row operations. Since the rank of U is m, each row of U' contains the leading 1, which is the only nonzero entry in its column. Let the rows of U' be $\mathbf{u}'_1, \ldots, \mathbf{u}'_m$ and let $\mathbf{x} = \mathbf{u}'_1 + \ldots + \mathbf{u}'_m$. Then $\mathbf{x} \in V$ and $\mathrm{wt}(\mathbf{x}) \ge m$. ∎

Let $\ell = \mathbb{Z}\text{-span}_n(\mathbf{v}_1, \ldots, \mathbf{v}_g) \subset I_g$ be a $\mathbb{Z}$-sublattice of rank n. Let $H = \{i_1, \ldots, i_h\} \subset G = \{1, \ldots, g\}$. We define

$$\ell_H := \mathbb{Z}\text{-span}_n(\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_h}) \subset I_h. \tag{14}$$

Note that the rank of ℓ_H is obviously less than or equal to $\min\{n, h\}$ and that ℓ_H is not necessarily a sublattice of ℓ.

LEMMA 2.2. *For a sublattice $\ell \subset I_g$ of rank n with $g > n(n+1)/2$, there exists an $H \subset G$ such that*

$$|H| \le \frac{n(n+1)}{2} \quad \textit{and} \quad \mathfrak{s}(\ell_{H'}) \subset 2\mathbb{Z},$$

where H' is the complement of H in G.

Proof. Put $\ell = \mathbb{Z}\text{-span}_n(\mathbf{v}_1, \dots, \mathbf{v}_g)$, where $\mathbf{v}_j = {}^{\mathrm{t}}(a_{1j}, \dots, a_{nj})$. We define a group homomorphism

$$\Phi(\ell) : \mathbb{F}_2^g \to \mathrm{Sym}_n(\mathbb{F}_2) \tag{15}$$

such that the (i,j)-entry of $\Phi(\ell)(s_1, \dots, s_g)$ is $\sum_{k=1}^{g} s_k a_{ik} a_{jk} \pmod 2$ for all $1 \le i, j \le n$. Note that if we let

$$V_\ell = \begin{pmatrix} a_{11} & \dots & a_{1g} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{ng} \end{pmatrix},$$

then

$$\Phi(\ell)(s_1, \dots, s_g) \equiv V_\ell \begin{pmatrix} s_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & s_g \end{pmatrix} {}^{\mathrm{t}}V_\ell \pmod 2.$$

Since $\dim(\mathrm{Sym}_n(\mathbb{F}_2)) = n(n+1)/2$, we get

$$\dim(\ker(\Phi(\ell))) \ge g - n(n+1)/2.$$

Hence there exists an $\mathbf{x} \in \ker(\Phi(\ell))$ such that

$$\mathrm{wt}(\mathbf{x}) \ge g - n(n+1)/2$$

by Lemma 2.1. Let H be the set of all indices i for which the ith component of $\mathbf{x}$ is zero. Then $|H| \le n(n+1)/2$ and $\mathfrak{s}(\ell_{H'}) \subset 2\mathbb{Z}$ as desired. ∎

Any sublattice ℓ of $L \perp M$ is of the form

$$\ell = \mathbb{Z}(\mathbf{x}_1 + \mathbf{y}_1) + \dots + \mathbb{Z}(\mathbf{x}_n + \mathbf{y}_n)$$

for $\mathbf{x}_i \in L$ and $\mathbf{y}_i \in M$. We define sublattices

$$\begin{aligned} \ell(L) &:= \mathbb{Z}\mathbf{x}_1 + \dots + \mathbb{Z}\mathbf{x}_n \subset L, \\ \ell(M) &:= \mathbb{Z}\mathbf{y}_1 + \dots + \mathbb{Z}\mathbf{y}_n \subset M. \end{aligned} \tag{16}$$

Even when $\sigma : \ell \to L \perp M$, we use $\ell(L)$ and $\ell(M)$ instead of $\sigma(\ell)(L)$ and $\sigma(\ell)(M)$, respectively, by abuse of notation.

LEMMA 2.3. *For $n = 7, 8$, let ℓ be the $\mathbb{Z}$-lattice of rank n such that the rank of the unimodular component of ℓ_2 in 2-adic Jordan decomposition is less than or equal to $11 - n$. Then $\ell \to I_{n+3}$.*

Proof. We prove only the case when $n = 7$. The other case can be proved in a similar manner. Let $(\ell_2)_0$ be the unimodular component of ℓ_2 in 2-adic

Jordan decomposition. If the rank of $(\ell_2)_0$ is ≤ 5 and $\ell \to E_8$, then $\ell \to I_8$ by Theorem 2 of [O'M2]. Recall the following fact:

$$\mathrm{gen}(I_{10}) = \{I_{10}, E_8 \perp I_2\}.$$

Since ℓ_p is represented by $(I_{10})_p$ for every p, ℓ is represented by $\mathrm{gen}(I_{10})$, which means ℓ is represented by either I_{10} or by $E_8 \perp I_2$. Suppose $\ell \to E_8 \perp I_2$. We may further assume that $\ell = \mathbb{Z}\mathbf{z}_1 + \ldots + \mathbb{Z}\mathbf{z}_7 \subset E_8 \perp I_2$, where $\mathbf{z}_i = \mathbf{x}_i + (a_{i1}\mathbf{e}_1 + a_{i2}\mathbf{e}_2)$ with $\mathbf{x}_i \in E_8, a_{i1}\mathbf{e}_1 + a_{i2}\mathbf{e}_2 \in I_2$ for all i, and that $B(\mathbf{z}_i, \ell) \equiv 0 \pmod 2$ for $1 \le i \le 3$. So, the rank of $(\ell(E_8)_2)_0 \le 5$ and hence $\ell(E_8) \to I_8$. This implies $\ell \to I_{10}$. ∎

3. Bounds of $g[n]$ for $7 \le n \le 20$. In this section, we provide bounds of $g[n]$ for small n's, which improves Sasaki's bounds.

THEOREM 3.1. *For* $7 \le n \le 11$,

$$g[n] \le n(n+1)/2 + n + 3.$$

Proof. Let $\ell \subset I_g$ be a $\mathbb{Z}$-sublattice of rank n, where $g > n(n+1)/2$. Let H, H' be the subsets of G satisfying the conditions in Lemma 2.2. Since $\phi(2) = 12$, every $\mathbb{Z}$-lattice of rank n is represented by $(1/\sqrt{2})I_{n+3}$. So, $\mathfrak{s}(\ell_{H'}) \subset 2\mathbb{Z}$ implies $\ell_{H'} \to I_{n+3}$. The theorem follows immediately. (See [Oh].) ∎

Note that the above proof cannot be applied to higher ranks because $\phi(2) = 12$. For $12 \le n \le 20$, let $\alpha(n), \beta(n)$ be integers satisfying

$$\binom{\alpha(n)}{1} + \binom{\alpha(n)}{2} + \ldots + \binom{\alpha(n)}{\beta(n)} \ge 2^{n(n+1)/2}. \tag{17}$$

THEOREM 3.2. *For* $12 \le n \le 20$,

$$g[n] \le n(n+1)\beta(n) + \alpha(n) + n + 2$$

where $\alpha(n), \beta(n)$ are any integers satisfying inequality (17).

Proof. Let $\ell \in \mathfrak{S}_n$ such that $\ell \subset I_g$. Then we may write ℓ as in (10). By (17) and the pigeonhole principle applied to $\mathrm{Sym}_n(\mathbb{F}_2)$ via the map $\Phi(\ell)$ of (15), we may assume that

$$\ell = \mathbb{Z}\text{-span}_n(\mathbf{u}_1, \ldots, \mathbf{u}_t, \mathbf{v}_{11}, \ldots, \mathbf{v}_{1j_1}, \ldots, \mathbf{v}_{s1}, \ldots, \mathbf{v}_{sj_s}),$$

where $\mathfrak{s}(\mathbb{Z}\text{-span}_n(\mathbf{v}_{k1}, \mathbf{v}_{k2}, \ldots, \mathbf{v}_{kj_k})) \subset 2\mathbb{Z}$, $1 \le j_k \le 2\beta(n)$ for all $k = 1, \ldots, s$, and $0 \le t \le \alpha(n) - 1$. Note that $t + j_1 + \ldots + j_s = g$. Here, s may be 0, which makes $t = g \le \alpha(n) - 1$. So, we may assume that $s \ne 0$. For each $\ell_k = \mathbb{Z}\text{-span}_n(\mathbf{v}_{k1}, \mathbf{v}_{k2}, \ldots, \mathbf{v}_{kj_k})$, $1 \le k \le s$, we let $2M_k$ be the corresponding symmetric matrix. Define

$$\Phi : \mathbb{F}_2^s \to \mathrm{Sym}_n(\mathbb{F}_2) \quad \text{by} \quad \Phi((\alpha_1, \ldots, \alpha_s)) = \sum_{k=1}^{s} \alpha_k M_k.$$

Then by a similar reasoning to Lemma 2.2, we may conclude that there exists a subset $K \subset \{(1,1),\dots,(1,j_1),(2,1),\dots,(2,j_2),\dots,(s,1),\dots,(s,j_s)\}$ such that

$$|K| \le n(n+1)\beta(n) \quad \text{and} \quad \mathfrak{s}((\ell_1 \perp \dots \perp \ell_s)_{K'}) \subset 4\mathbb{Z},$$

where

$$\ell_1 \perp \dots \perp \ell_s = \mathbb{Z}\text{-span}_n(\mathbf{v}_{11},\dots,\mathbf{v}_{1j_1},\mathbf{v}_{21},\dots,\mathbf{v}_{2j_2},\dots,\mathbf{v}_{s1},\dots,\mathbf{v}_{sj_s}).$$

Therefore the desired inequality follows from Theorem 18 of [CS2]. ∎

REMARK. The inequality (17) is satisfied by $\alpha(n)=n^3, \beta(n)=\lfloor 13n/10\rfloor$ for $12 \le n \le 20$. So, from Theorem 3.2 it follows that

$$g[n] < 5n^3/2 \tag{18}$$

for $12 \le n \le 20$.

4. Sharper bounds for $g[7]$ and $g[8]$. In this section, we restrict ourselves to the case when $n = 7$ or 8.

THEOREM 4.1. *We have*

$$11 \le g[7] \le 24.$$

Proof. The lower bound comes from (4). Let $\ell = \mathbb{Z}\mathbf{x}_1 + \dots + \mathbb{Z}\mathbf{x}_7 \subset I_g$ for sufficiently large g, where $\mathbf{x}_i = (a_{i1},\dots,a_{ig})$ for $1 \le i \le 7$. Let $\mathbf{v}_j = {}^{\mathrm{t}}(a_{1j},\dots,a_{7j})$ for $1 \le j \le g$ so that $\ell = S_7(\mathbf{v}_1,\dots,\mathbf{v}_g) \subset I_g$. For a subset $T = \{t_1,\dots,t_5\} \subset S = \{1,\dots,7\}$, we define a sublattice

$$\ell^T := \mathbb{Z}\mathbf{x}_{t_1} + \dots + \mathbb{Z}\mathbf{x}_{t_5}$$

of ℓ and let $\mathbf{v}_j^T := {}^{\mathrm{t}}(a_{t_1 j}, a_{t_2 j}, \dots, a_{t_5 j})$. Then by Lemma 2.2, there exists a subset H such that $|H| \le 15$ and $\mathfrak{s}(\ell_{H'}^T) \subset 2\mathbb{Z}$. Note that $\ell_{H'}^T \subset \ell_{H'}$. After a suitable base change, this implies that

$$M_{\ell_{H'}} \equiv \begin{pmatrix} 0&0&0&0&0&*&*\\ 0&0&0&0&0&*&*\\ 0&0&0&0&0&*&*\\ 0&0&0&0&0&*&*\\ 0&0&0&0&0&*&*\\ *&*&*&*&*&*&*\\ *&*&*&*&*&*&* \end{pmatrix} \pmod 2.$$

Therefore the rank of the unimodular component of $(\ell_{H'})_2$ is less than or equal to 4. Hence by Lemma 2.3,

$$\ell \to \ell_{H'} \perp I_{15} \to I_{25}.$$

We now fix $g = 25$ so that $\ell = S_7(\mathbf{v}_1,\dots,\mathbf{v}_{25})$. We may assume that ℓ is a primitive sublattice of I_{25}. Suppose that ℓ is not represented by I_{24}. Then

for any subset $T \subset S$ with $|T| = 5$, we have

$$\dim(\Phi(\ell^T)(\mathbb{F}_2^{25})) = 15, \quad \dim(\ker(\Phi(\ell^T))) = 10,$$

and the maximal weight among the vectors in $\ker(\Phi)$ must be 10. So, we may further assume that $\Phi(\ell^T)(\mathbf{e}_j)$'s for $1 \le j \le 15$ form a basis of $\mathrm{Sym}_5(\mathbb{F}_2)$ and

$$\sum_{k=16}^{25} \Phi(\ell^T)(\mathbf{e}_k) = 0.$$

For each $16 \le k_0 \le 25$,

$$\Phi(\ell^T)(\mathbf{e}_{k_0}) = \sum_{k \ne k_0} \Phi(\ell^T)(\mathbf{e}_k) = \sum_{j=1}^{15} a_j \Phi(\ell^T)(\mathbf{e}_j)$$

implies that $\Phi(\ell^T)(\mathbf{e}_{k_0})$ is either 0 or $\Phi(\ell^T)(\mathbf{e}_j)$ for some $1 \le j \le 15$. Consequently, there are exactly 15 distinct non-zero vectors in $\{\mathbf{v}_1^T, \dots, \mathbf{v}_{25}^T\}$ $(\mathrm{mod}\, 2)$ and the number of the same non-zero vectors $(\mathrm{mod}\, 2)$ in the set is always odd.

We now show that there exists a set T violating the above condition. Note that $\sum_{r \in R} \mathbf{x}_r \not\equiv \mathbf{0} \pmod 2$ for any subset $R \subset \{1, \dots, 7\}$. We may choose $T = \{1, \dots, 5\}$ and assume that $\Phi(\ell^T)(\mathbf{e}_j)$'s for $1 \le j \le 15$ form a basis of $\mathrm{Sym}_5(\mathbb{F}_2)$. By a suitable base change and rearrangement, we may assume that for $1 \le j \le 5$,

$$\mathbf{v}_j \equiv \mathbf{f}_j, \quad \mathbf{v}_{24} \equiv \mathbf{f}_6, \quad \mathbf{v}_{25} \equiv \mathbf{f}_7 \pmod 2,$$

where $\mathbf{f}_j$ is the transpose of the jth standard basis vector of $\mathbb{F}_2^7$.

Table 4.1

$$\begin{aligned}
\mathbf{x}_1 &\equiv 1,0,0,0,0,a_{16},\dots,a_{1,15};\ a_{1,16},\dots,a_{1,23},0,0 \pmod 2\\
\mathbf{x}_2 &\equiv 0,1,0,0,0,a_{26},\dots,a_{2,15};\ a_{2,16},\dots,a_{2,23},0,0 \pmod 2\\
\mathbf{x}_3 &\equiv 0,0,1,0,0,a_{36},\dots,a_{3,15};\ a_{3,16},\dots,a_{3,23},0,0 \pmod 2\\
\mathbf{x}_4 &\equiv 0,0,0,1,0,a_{46},\dots,a_{4,15};\ a_{4,16},\dots,a_{4,23},0,0 \pmod 2\\
\mathbf{x}_5 &\equiv 0,0,0,0,1,a_{56},\dots,a_{5,15};\ a_{5,16},\dots,a_{5,23},0,0 \pmod 2\\
\hline
\mathbf{x}_6 &\equiv 0,0,0,0,0,a_{66},\dots,a_{6,15};\ a_{6,16},\dots,a_{6,23},1,0 \pmod 2\\
\mathbf{x}_7 &\equiv 0,0,0,0,0,a_{76},\dots,a_{7,15};\ a_{7,16},\dots,a_{7,25},0,1 \pmod 2
\end{aligned}$$

Note that for every j, $6 \le j \le 15$, there exists an i, $1 \le i \le 4$, such that $a_{ij} \not\equiv 0 \pmod 2$. For each given j, $1 \le j \le 5$, the number of k's, $16 \le k \le 23$, such that $\mathbf{v}_k^T \equiv \mathbf{f}_j^T \pmod 2$ is even. Hence we may assume that

$$\text{if} \quad a_{5k} \equiv 1 \pmod 2, \quad \text{then} \quad a_{ik} \equiv 1 \pmod 2$$

for at least one i, $1 \le i \le 4$. Let a, b, c, d be the numbers of $\mathbf{v}_k$'s, $16 \le k \le 23$, such that

$$\mathbf{v}_k = \mathbf{0}, \quad \mathbf{v}_k = \mathbf{f}_6, \quad \mathbf{v}_k = \mathbf{f}_7, \quad \mathbf{v}_k = \mathbf{f}_6 + \mathbf{f}_7,$$

respectively. If we replace $\mathbf{x}_5$ by $\mathbf{x}_5 + \mathbf{x}_6$ or $\mathbf{x}_5 + \mathbf{x}_7$, then the number of j's, $1 \le j \le 25$, such that $\mathbf{v}_j^T \equiv \mathbf{f}_5^T \pmod 2$ has to be odd. Therefore

$$a + b + c + d \equiv 0, \quad b + d + 1 \equiv 1, \quad c + d + 1 \equiv 1 \pmod 2. \tag{19}$$

Since (19) holds for any choice of T, either the number of j's such that $\mathbf{v}_j = \mathbf{f}_k$ is always even for any $k, 1 \le k \le 7$, or the number of j's such that $\mathbf{v}_j = \mathbf{f}_k$ is always odd for any $k, 1 \le k \le 7$, and there exists $\mathbf{v}$ such that $\mathbf{v} = \mathbf{f}_k + \mathbf{f}_l$ for any k, l, $1 \le k, l \le 7$. Note that the latter case cannot occur. In the former case, there exists an $H \subset \{1, \dots, 25\}$ such that $|H| \le 11$ and $\mathfrak{s}(\ell_{H'}) \subset 2\mathbb{Z}$. This implies $\ell \to I_{21}$, which is not possible either. ∎

THEOREM 4.2.

$$13 \le g[8] \le 37.$$

Proof. The lower bound comes from (4). Let $\ell = S_8(\mathbf{v}_1, \dots, \mathbf{v}_g) \subset I_g$ be of rank 8. Let

$$W := \{M = (m_{ij}) \in \mathrm{Sym}_7(\mathbb{F}_2) \mid m_{ij} = 0 \text{ if } (i,j) \ne (7,7)\}.$$

For any subset $T \subset \{1, \dots, 8\}$ with $|T| = 7$, we can define a linear map

$$\Phi(\ell^T) : \mathbb{F}_2^g \to \mathrm{Sym}_7(\mathbb{F}_2)/W$$

via factoring the map defined in (15). Note that $\dim(\mathrm{Sym}_7(\mathbb{F}_2)/W) = 27$. Then by a similar reasoning to Lemma 2.2, one can show that there exists a subset $H \subset G = \{1, \dots, g\}$ with $|H| \le 27$ such that the rank of the unimodular component of $(\ell_{H'})_2$ is less than or equal to 3. Therefore by Lemma 2.3, $\ell_{H'} \to I_{11}$ and hence $\ell \to I_{38}$. The rest (for improving the upper bound by 1) is almost identical to the case when $n = 7$. ∎

References

[CS1] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer, 1999.

[CS2] —, —, *Low dimensional lattices V. Integral coordinates for integral lattices*, Proc. Roy. Soc. London Ser. A 426 (1989), 211–232.

[HKK] J. S. Hsia, Y. Kitaoka and M. Kneser, *Representation of positive definite quadratic forms*, J. Reine Angew. Math. 301 (1978), 132–141.

[Ic] M. I. Icaza, *Sums of squares of integral linear forms*, Acta Arith. 74 (1996), 231–240.

[KKO] B. M. Kim, M.-H. Kim and B.-K. Oh, *2-universal positive definite integral quinary quadratic forms*, in: Contemp. Math. 249, Amer. Math. Soc., 1999, 51–62.

[KO1] M.-H. Kim and B.-K. Oh, *A lower bound for the number of squares whose sum represents integral quadratic forms*, J. Korean Math. Soc. 33 (1996), 651–655.

[KO2] M.-H. Kim and B.-K. Oh, *Representation of positive definite senary integral quadratic forms by a sum of squares*, J. Number Theory 63 (1997), 89–100.

[KO3] —, —, *Representation of integral quadratic forms by sums of squares*, preprint.

[K1] C. Ko, *On the representation of a quadratic form as a sum of squares of linear forms*, Quart. J. Math. Oxford 8 (1937), 81–98.

[K2] —, *On the decomposition of quadratic forms in six variables*, Acta Arith. 3 (1939), 64–78.

[L] J. L. Lagrange, *Oeuvres*, *III*, Paris, 1869, 189–201.

[M1] L. J. Mordell, *A new Waring's problem with squares of linear forms*, Quart. J. Math. Oxford 1 (1930), 276–288.

[M2] —, *The representation of a definite quadratic form as a sum of two others*, Ann. of Math. 38 (1937), 751–757.

[Oh] B.-K. Oh, *On universal forms*, Ph.D. thesis, Seoul National Univ., 1999.

[O'M1] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer, 1973.

[O'M2] —, *The integral representations of quadratic forms over local fields*, Amer. J. Math. 80 (1958), 843–878.

[Pl] W. Plesken, *Additively indecomposable positive integral quadratic forms*, J. Number Theory 47 (1994), 273–283.

[Sa] H. Sasaki, *Sums of squares of integral linear forms*, J. Austral. Math. Soc. Ser. A 69 (2000), 298–302.

School of Mathematics
Seoul National University
Seoul 151-742, South Korea
E-mail: mhkim@math.snu.ac.kr

Department of Mathematics
Ohio State University
Columbus, OH 43210, U.S.A.
E-mail: bkoh@ohio-state.edu

Received on 28.3.2001
and in revised form on 10.12.2001 (4008)